Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Sahoo, Liu, dan Hoi (2017) berpendapat bahwa perkembangan teknologi komunikasi telah membantu untuk memajukan bisnis seperti *online-banking*, *e-commerce*, dan promosi melalui *social networking*. Perkembangan teknologi komunikasi juga memberi dampak dalam bidang sosial, seperti media sosial yang sering digunakan untuk berkomunikasi dan berbagi cerita (Dhawan, Singh, dan Divya, 2016).

Namun, selain membantu dalam memajukan bisnis, perkembangan teknologi komunikasi juga menciptakan peluang bagi pelaku kriminal untuk menyerang dan menipu banyak orang dengan menggunakan cara-cara canggih (Ma, Saul, Savage, dan Voelker, 2009; Sahoo dkk., 2017). Salah satu cara tersebut adalah *phishing*. Weedon, Tsaptsinos, dan Denholm-Price (2017) mendefinisikan *phishing* sebagai "sebuah metode yang digunakan kriminal untuk menipu dan mengecoh pengguna agar memberikan data personal dan sensitif, seperti identitas diri dan informasi finansial". Weedon dkk. (2017) menyatakan adanya peningkatan jumlah situs *phishing* dari bulan Oktober tahun 2015 sampai bulan Juni tahun 2016 sebanyak 466.065 situs atau sebesar 61%. Gudvoka, Vergelis, Shcherbakova, dan Demidova (2018, Februari 15) menyatakan bahwa pada tahun 2017, sistem anti-*phishing* Kapersky Lab yang terdapat di komputer pengguna sudah melakukan 246.231.645 kali usaha untuk mencegah redireksi dari *phishing*. Dari data-data tersebut, terbukti bahwa masih banyak usaha *phishing* yang dilakukan kriminal.

Kriminal dapat melakukan *phishing* dengan cara menyebarkan URL (*Uniform Resource Locator*) melalui internet seperti forum dan *private message*, melalui situs web seperti *blog*, dan mengirim *e-mail* kepada korban dengan cara menyamar memakai nama instansi terkenal atau

nama seseorang yang dapat dipercaya oleh korban (Basnet dan Doleck, 2015; Weedon dkk., 2017; Basnet, Sung, dan Liu, 2014). Dalam cara-cara tersebut, URL yang dikirim mengarah ke situs web *phishing* yang meminta korban untuk memasukkan identitas diri dan data finansial. Setelah itu, kriminal mendapatkan data dan menggunakannya untuk melakukan tindakan kriminal seperti melakukan akses ilegal dan menyamar dengan menggunakan identitas korban.

Menurut Basnet dan Doleck (2015), cara yang paling sering dipakai *browser* untuk menghindari *phishing* adalah dengan melakukan *blacklisting*. *Blacklist* adalah kumpulan URL yang terbukti merupakan *phishing* URL (Sahoo dkk., 2017). Dengan adanya *blacklist*, *phishing* URL bisa disaring sehingga pengguna dapat menghindari usaha *phishing*. Daftar URL yang terdapat pada *blacklist* dapat diisi dengan menggunakan cara seperti *honeypots*, *web crawlers*, dan URL yang dilaporkan pengguna internet sebagai *phishing* (Weedon dkk., 2017). Namun, menurut Weedon dkk. (2017), cara tersebut tidak bisa menangani semua URL yang berbahaya karena tidak *up-to-date* dengan data URL terbaru dan tidak dievaluasi dengan baik.

Solusi yang diterapkan selain melalui *blacklist* adalah dengan menggunakan *machine learning*. Weedon dkk. (2017) menggunakan algoritma Random Forest untuk mengklasifikasi URL *phishing* dengan basis leksikal, yaitu *feature* yang digunakan untuk *training* diambil dari URL itu sendiri. Dhawan dkk. (2016) juga menggunakan algoritma Random Forest untuk mengklasifikasi *malicious* URL pada Twitter.

Weedon dkk. (2017) menemukan bahwa klasifikasi *phishing* URL dengan algoritma Random Forest (RF) memiliki akurasi sebesar 86.9% dibandingkan menggunakan algoritma Naïve Bayes (NB), Logistic Regression (LR), dan J48 yang secara berurutan memiliki akurasi 64.6%, 81.5%, dan 83.9%. Selain itu, dengan RF, jumlah *false negatives* yang dihasilkan sebesar 782, lebih sedikit dari algoritma NB, LR, dan J48 yang secara berurutan menghasilkan *false negatives*

sebesar 2412, 1180, dan 1002. Nilai *false negatives* yang kecil penting karena jika URL yang *phishing* diklasifikasi sebagai tidak *phishing*, maka potensi untuk membahayakan pengguna lebih besar. Basnet, Sung, dan Liu (2014) juga menemukan bahwa hasil evaluasi klasifikasi *phishing* URL dengan algoritma RF, J48, Multilayer Perceptron, LR, Support Vector Machine (SVM) dengan kernel linear, SVM dengan kernel RBF, dan NB, secara keseluruhan, algoritma RF memiliki performa paling baik di antara algoritma-algoritma lain dalam hal *overall error rates*, *false positive rates*, dan *false negative rates*.

Menurut Kyriakopoulou dan Kalamboukis (2006), sebelum melakukan klasifikasi, *classifier* idealnya mengetahui informasi mengenai persebaran *testing data*. Oleh sebab itu, Kyriakopoulou dkk. (2006) mengajukan algoritma yang mengkombinasikan teknik *supervised learning* dan *unsupervised learning*. Algoritma tersebut digunakan pada eksperimen dalam pembuatan sebuah *spam filter classifier* dengan menggunakan algoritma SVM dan TSVM. Hasilnya, algoritma SVM dan TSVM menghasilkan nilai AUC (*Area Under Curve*) yang lebih besar jika dikombinasikan dengan *clustering*. Feroz dan Mengel (2015) juga melakukan proses *clustering* dan menggunakan *cluster id* yang didapat sebagai *predictor variable* atau *feature* tambahan untuk klasifikasi.

Salah satu algoritma *unsupervised learning* yang dipakai untuk *clustering* adalah K-Means. Menurut Farhang (2017), algoritma K-Means Clustering cocok untuk mengklasterisasi kumpulan data yang besar karena sederhana dan cepat. Arthur dan Vassilvitskii (2007) mengajukan teknik untuk memasukkan *centroid* awal untuk algoritma K-Means. Dalam eksperimennya, teknik tersebut dapat menghasilkan akurasi dan kecepatan proses yang lebih baik. Teknik tersebut digabung dengan K-Means dipanggil dengan sebutan K-Means++. Baykal dkk. (2016) menggunakan K-Means++ untuk membuat *image forgery detection*. Öztürk dkk. (2015)

juga menggunakan K-Means++ untuk membuat *defect prediction* untuk halaman web. Dari latar belakang masalah yang telah dijelaskan, algoritma K-Means++ dan Random Forest digunakan untuk klasifikasi *phishing* URL.

1.2 Rumusan Masalah

Rumusan masalah penelitian ini berdasarkan latar belakang tersebut adalah sebagai berikut.

1. Bagaimana mengimplementasikan algoritma K-Means++ Clustering dan Random Forest untuk klasifikasi *phishing* URL?
2. Berapa akurasi yang dihasilkan algoritma K-Means++ Clustering dan Random Forest untuk klasifikasi *phishing* URL?

1.3 Batasan Masalah

Batasan masalah penelitian ini adalah sebagai berikut.

1. Kumpulan data yang digunakan sebagai *training data* dan *testing data* didapat dari situs web PhishTank untuk *phishing* URL dan data yang didapat dari situs web DMOZ untuk bukan *phishing* URL.
2. URL yang dihasilkan dari *service* seperti URL *shorterner* tidak termasuk dalam data.
3. *Feature extraction* hanya diambil dari *string* URL atau *lexical based*.
4. Jumlah *decision tree* yang dibuat dalam Random Forest adalah 100.
5. *Splitting criteria* yang digunakan saat membuat *decision tree* adalah *gini index*.

1.4 Tujuan Penelitian

Tujuan penelitian berdasarkan rumusan masalah yang sudah dibuat adalah mengimplementasikan algoritma K-Means++ Clustering dan Random Forest dalam

UNIVERSITAS MULTIMEDIA NUSANTARA

mengklasifikasikan *phishing* URL dan menghitung akurasi yang dihasilkan algoritma K-Means++ Clustering dan Random Forest untuk klasifikasi *phishing* URL.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

1.5 Manfaat Penelitian

Manfaat yang bisa didapatkan dari penelitian ini adalah sebagai berikut.

1. Memberi sumbangan ilmu pengetahuan mengenai K-Means++ Clustering dalam penerapannya untuk *clustering phishing* URL dan menggunakan hasil *clustering* sebagai *feature* tambahan untuk klasifikasi.
2. Membuat sebuah sistem klasifikasi yang dapat digunakan untuk mendeteksi *phishing* URL supaya pengguna dapat terhindar dari *phishing* URL.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA